

11 DECEMBER 2000



Communications and Information

**COMMUNICATIONS SECURITY:
PROTECTED DISTRIBUTION SYSTEMS (PDS)**

NOTICE: This publication is available digitally on the AFDPO WWW site at: <http://afpubs.hq.af.mil>.

OPR: HQ AFCA/TCBA (Mr. Dwight Bohl)

Certified by: Certified: HQ USAF/SCXX
(Col Terry G. Pricer)

Pages: 30

Distribution: F

This Air Force manual (AFMAN) prescribes the construction and approval requirements for a protected distribution system (PDS) and implements National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protected Distribution Systems*, and Air Force Policy Directive (AFPD) 33-2, *Information Protection* (will convert to *Information Assurance*). We encourage you to use extracts from this manual. Air Force Directory (AFDIR) 33-303, *Compendium of Communications and Information Terminology*, explains other terms. Direct questions or comments on the contents of this publication to Headquarters, Air Force Communications Agency, (HQ AFCA/ITPP), 203 W. Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**. Send an information copy to HQ AFCA/TCBA, 203 W. Losey Street, Room 2000, Scott AFB IL 62225-5222, and HQ USAF/SCMI, 1250 Air Force Pentagon, Washington DC 20330-1250. A glossary of references and supporting information is at **Attachment 1**. Maintain and dispose of all records created as a result of prescribed processes in accordance with AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322, Volume 4).

This AFMAN replaces Air Force Systems Security Instruction (AFSSI) 3030, Communications Security: Protected Distribution Systems (PDS), dated 1 May 1997.

1.	Introduction	2
2.	Protected Distribution System Defined	3
3.	Protected Distribution System Selection Considerations	3
4.	Protected Distribution System Justification	4
5.	Protected Distribution System Plan	4
6.	Protected Distribution System Plan Validation	5
7.	Protected Distribution System Construction	6
8.	Protected Distribution System Certification	6

Report Documentation Page

Report Date 11 Dec 2000	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Air Force Instruction 33-221, Communications and Information Communications Security: Protected Distribution Systems (PDS)		Contract Number
		Grant Number
		Program Element Number
Author(s)		Project Number
		Task Number
		Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250		Performing Organization Report Number AFI33-221
Sponsoring/Monitoring Agency Name(s) and Address(es)		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified		Classification of this page unclassified
Classification of Abstract unclassified		Limitation of Abstract UU
Number of Pages 30		

9.	Protected Distribution System Approval	6
10.	Protected Distribution System Recertification	7
Figure 1.	The PDS Package File	8
11.	Protected Distribution System Deactivation	8
12.	Information Collections, Records, and Forms	8
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		9
Attachment 2—PROTECTED DISTRIBUTION SYSTEMS PROCESS Flow Chart		11
Attachment 3—PROTECTED DISTRIBUTION SYSTEMS OPERATION REQUIREMENTS		12
Attachment 4—PROTECTED DISTRIBUTION SYSTEMS PHYSICAL SECURITY REQUIREMENTS		14
Attachment 5—PROTECTED DISTRIBUTION SYSTEM SIGNAL LINE REQUIREMENTS		20
Attachment 6—PROTECTED DISTRIBUTION SYSTEMS CONSTRUCTION REQUIREMENTS		22
Attachment 7—PROTECTED DISTRIBUTION SYSTEMS CIRCUIT SEPARATION REQUIREMENTS		28
Attachment 8—PROTECTED DISTRIBUTION SYSTEMS TECHNICAL INSPECTIONS		29

1. Introduction . Air Force Instruction (AFI) 33-201, (FOUO) *Communications Security (COMSEC)*, requires the use of National Security Agency (NSA)-endorsed communications security (COMSEC) products and services to secure classified telecommunications by all Air Force activities and their contractors. Information systems or networks that process classified national security information in more than one controlled access area (CAA) and require the transfer of that information between CAAs, must use a secure means of transference--secure telecommunications or courier. If secure telecommunications is chosen, include a secure telecommunications requirement (COMSEC) in the systems security policy. In order of preference, the COMSEC requirement is met by: NSA-endorsed COMSEC systems (encryption), NSA-endorsed intrusion detection optical communications system (IDOCs), or a protected distribution system (PDS). AFI 33-201 also requires the use of NSA-endorsed COMSEC products, techniques, and protected services to protect certain unclassified, sensitive telecommunications involving Air Force activities and their contractors. When certain unclassified, sensitive information must be protected, and a PDS is chosen, follow the standards in this manual for CONFIDENTIAL information. At [Attachment 2](#) is a flow chart of the process to design, construct, approve, and operate a PDS.

1.1. Although it is the last alternative for consideration, you may use a PDS to transmit unencrypted, clear-text, classified national security information if the PDS provides adequate electrical, electromagnetic, physical, and procedural safeguards identified in this manual. In establishing the standards for PDS construction and use, national managers incorporated the philosophy of risk management rather than risk avoidance. As such, the standards specified in this manual are the minimum protection standards based on national guidance. The assumption of any additional risk to lessen the minimum specified standards is not an option. Organizations wishing to discuss this policy may forward their specific concerns through command channels to HQ AFCA/GCI. Develop the technical solution using the process described in AFI 33-103, *Requirements Development and Processing*, to justify a PDS. Use of any PDS not meeting the standards of this manual is prohibited.

1.2. Do not use a PDS within a high threat environment as defined by NSTISSI 7000, (C) *TEMPEST Countermeasures for Facilities* (U), Annex A, (S) *TEMPEST Threat to Facilities* (U). Major command (MAJCOM) information assurance (IA) offices are on automatic distribution for this document.

2. Protected Distribution System Defined . A PDS is a physically protected signal line (wire or fiber optic) between subscribers who electronically share classified national security information and certain unclassified, sensitive information.

2.1. Those subscribers that share classified national security information reside in CAAs and the PDS protects information passed between them through areas of lesser control. A CAA processing the classified information can be a desk, cubicle, set of cubicles, room, group of rooms, wing, floor, building, or buildings.

2.2. Establishing or defining both CAA boundaries is important because a PDS is installed between CAAs, not within a CAA, although the PDS may extend into the CAA. A signal line carrying classified information within the CAA is considered a RED signal line.

2.3. In short, a PDS is the signal line carrying classified information and the distribution system comprised of either a hardened or simple distribution system (see [Attachment 4](#) and [Attachment 6](#)) providing the acceptable degree of physical security to the signal line.

2.4. Do not run BLACK signal wire lines in a PDS with RED signal wire lines because of crosstalk. BLACK fiber optic signal lines may be run in a PDS with RED signal lines, but is discouraged for three reasons. It is difficult to identify BLACK signal lines anywhere within the PDS except at the ends. Any person with a need to access the BLACK signal lines must have the appropriate clearance or be escorted. All breakouts of BLACK signal lines must be made in a CAA.

3. Protected Distribution System Selection Considerations . The requesting agency, in concert with the communications and information systems officer (CSO) and systems telecommunications engineering manager (STEM), must carefully consider using a PDS before selecting it in preference to other COMSEC solutions. Economic, technical, or operational factors may make a PDS necessary in comparison to other COMSEC solutions. However, a PDS is not a preferred method and is considered only as a last resort.

3.1. Operation Considerations. Operating a PDS requires continued physical security integrity after construction. The cost and operational impact of maintaining the security of the system can easily exceed the construction costs. Consider using a PDS only after the requesting agency agrees to provide it the required degree of protection 24 hours a day, 7 days a week.

3.2. **Classification Level Considerations.** When reviewing communications needs, consider future requirements in regard to the classification level of the information to be transmitted, the requisite physical controls needed, and the geographical location of the PDS site. Typically it is easier and less costly to include the capability for future requirements than to retrofit an installed system for such updates.

3.3. **Physical Security Considerations.** The operating agency must follow normal procedures to protect the PDS terminal equipment and interconnecting signal lines within any adjoining CAA such that only persons who are cleared for the highest classification and category of information transmitted over the system may have unrestricted access to the system. Escort all personnel who do not have the appropriate security clearance, but require occasional, temporary access to the PDS terminal equipment and interconnecting lines (for example, safety and fire inspectors) to prevent a compromise of the information or the security integrity of the PDS. Maintain the physical security integrity of the PDS on a continual basis, regardless of whether the PDS is in continuous operation or not. The intent is to detect any signs of tampering or penetration as early as possible, and before the system is used again.

4. Protected Distribution System Justification . Justify a PDS using the technical solution process of AFI 33-103 and meet the requirements of this manual before approving construction or use. The requesting agency, CSO, and STEM must justify using a PDS instead of an approved COMSEC system, IDOCS, or courier before submitting the technical solution for approval.

4.1. Justify the PDS by:

4.1.1. Showing that courier is not timely, practical, or feasible.

4.1.2. Using a capability or cost basis.

4.2. If the justification is based on capability, the CSO must show:

4.2.1. There is no COMSEC system or IDOCS with the capability to handle the data to be passed over the PDS.

4.2.2. A capable COMSEC system exists; however, equipment is not available to support this requirement. IDOCS provides the capability to secure communications over optical fiber lines without the use of encryption or a PDS.

4.3. If the justification is based on cost, the requesting agency must clearly indicate a PDS is less costly than using an approved COMSEC system or IDOCS. When this justification is used, compare and show the total life-cycle cost of COMSEC equipment or IDOCS to the total life-cycle cost of the proposed PDS. As a minimum, the PDS plan must show the following:

4.3.1. PDS construction costs.

4.3.2. Annual operation and maintenance costs.

4.3.3. Annual physical security costs.

4.4. The justification is the first document of the PDS package file (see [Figure 1.](#)). A separate file is required for each PDS.

5. Protected Distribution System Plan . The requesting agency must prepare a PDS plan prior to constructing a PDS. Obtain a PDS identification number from the wing IA office. This number consists of

the MAJCOM, the base, and a unique three-digit number (for example, AMC-Scott-001). This plan identifies and assigns responsibility for operational security requirements and specifies the design and construction requirements.

5.1. Information and Access Requirements. Identify:

5.1.1. Highest classification level and category of information carried by the PDS.

5.1.2. Minimum security clearance level of individuals with unrestricted access to any portion of the PDS.

5.2. User Information. Identify:

5.2.1. Name and location of the requesting agency. This will normally be the office of record for the PDS. The office of record will maintain the PDS file.

5.2.2. Name, organization, and office symbol of the Designated Approving Authority (DAA) (see paragraph 9.).

5.2.3. CAAs (buildings and room numbers) connected by the PDS. There are three kinds of CAAs: open storage areas, secured facilities, and open offices that are locked at night and on weekends. The open offices present the most difficulties in meeting security requirements.

5.2.4. Organizations and office symbols occupying the CAAs identified in paragraph 5.2.3. connected by the PDS.

5.3. PDS Operation Requirements. Specify the operation requirements (see Attachment 3). Document each requirement with an official memorandum, a letter of appointment, an operating instruction, or other official means. Drafts are permitted for validation. Finalize drafts prior to certification.

5.4. PDS Physical Security Requirements. Identify the physical security requirements from Attachment 4.

5.5. PDS Signal Line Requirements. Identify the signal line requirements from Attachment 5.

5.6. PDS Construction Requirements. Identify the physical construction requirements from Attachment 6. Identify the organization proposed to install the PDS.

5.7. Circuit Separation Requirements. Refer to Attachment 7 for circuit separation criteria when sharing a single distribution system.

6. Protected Distribution System Plan Validation . The requesting agency submits a copy of the PDS justification and the PDS plan to the wing IA office for validation.

6.1. The wing IA office reviews the justification for adequacy and the plan for obvious errors such as requiring unnecessary redundancy in protection or any major omissions. If all the operational security requirements are met, the wing IA office validates the PDS plan and creates a PDS file. Place the PDS plan on top of the justification as part of the PDS file (see Figure 1.). The requesting agency may maintain a duplicate copy of the file.

6.2. Document the validation as a memorandum. Attach the validation to the PDS file (see Figure 1.).

6.3. The wing IA office keeps a copy of the PDS file to be used during certification.

6.4. Return the original file to the requesting agency.

6.5. When proposing a modification to an existing PDS, include only the items pertaining to the modification when requesting approval.

7. Protected Distribution System Construction . Construct the PDS according to the validated plan. Do not use the PDS to pass classified national security information until the PDS is approved by the DAA. Document all deviations. All members of the team constructing the PDS must have an appropriate security clearance to prevent any instance of “pretampering” of the system. If cleared personnel are not available they must be escorted at all times by someone from outside the team with an appropriate clearance. The escort must have sufficient technical knowledge to recognize any attempts of tampering or penetration.

8. Protected Distribution System Certification . After construction, the requesting agency requests certification from the wing IA office. Provide the wing IA office documentation for any deviations from the plan. The deviations become a part of the PDS plan and are attached to the plan. Include finalized instructions, memorandums, and letters of agreement. Replace the drafts with the final documents in the PDS file. The wing IA office reviews the plan and the deviations.

8.1. The wing IA office certifies:

- 8.1.1. Compliance with the construction plan, including deviations.
- 8.1.2. Successful completion of a lines route inspection, if required.
- 8.1.3. Alarm circuit verification procedures, if required.
- 8.1.4. Continuous viewing procedures, if required.
- 8.1.5. The PDS passed a technical inspection by the technical inspector.
- 8.1.6. The controlling office is identified.
- 8.1.7. The incident reporting and investigating system is in effect.

8.2. The wing IA office:

- 8.2.1. Ensures all discrepancies are corrected before certifying the PDS.
- 8.2.2. Documents the certification as a memorandum. Attaches the certification memorandum to the PDS file (see [Figure 1.](#)).
- 8.2.3. Keeps a copy and forwards the certification to the requesting agency.
- 8.2.4. Attaches any deviations and the certification to the PDS file (see [Figure 1.](#)).

9. Protected Distribution System Approval .

9.1. Approving the PDS. The requesting agency submits the PDS certification memorandum to the DAA. The DAA approves operation of the PDS as part of the system's certification and accreditation (C&A). The PDS file is independent of, but essential to, the system's C&A.

9.2. Filing the Approval. Forward a copy of the approval to the wing IA office for their files. The wing IA office attaches the PDS approval to the PDS file as shown in [Figure 1.](#)

9.3. Approving Authorities. Except as noted below, the DAA approves the PDS as a part of the C&A process for the network or information system the PDS is supporting. AFPD 33-2 requires that all sys-

tems be certified and accredited prior to operation. AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*, details the process that will be used to certify and accredit Air Force systems. Complete the requirements of AFSSI 5024 Volume 1 before getting approval to operate.

9.3.1. Temporary Systems. The developmental or systems DAA may approve temporary configurations without processing a formal approval package if the PDS:

9.3.1.1. Is in place no more than 1 month.

9.3.1.2. Is confined within U.S. Government installations.

9.3.1.3. Does not process higher than SECRET information.

9.3.2. Contractor Facilities. The head of the government contracting department or agency is the approving authority for a contractor-owned and operated PDS.

9.3.3. Tactical Systems. The developmental or systems program office approves a PDS used in a tactical system using intershelter cabling. Once approved, tactical systems do not require reapproval upon relocation provided the previously approved configuration is not changed (such as, the site physical security requirements, line lengths, cable types, connections, connectors, and so forth). A change in the physical placement of components is not a change in configuration.

9.3.4. Systems without a DAA. For those systems not requiring a DAA, e.g., radio transmit and receive lines, the approving authority is the unit commander.

10. Protected Distribution System Recertification .

10.1. The wing IA office recertifies a PDS as part of the system recertification and reaccreditation:

10.1.1. Every 3 years, if installed within the United States, its trust territories, and possessions (hereafter called the United States).

10.1.2. Annually, if installed outside the United States.

10.2. Recertify the PDS after verifying the following:

10.2.1. Lines route inspections (if needed) – the PDS meets requirements and previous inspections were completed on schedule.

10.2.2. Technical inspections – the PDS was within limits and the inspections were completed on schedule (see [Attachment 8](#)).

10.2.3. Alarm circuit (if used) verification – previous alarm circuit tests were successful and completed on schedule.

10.2.4. PDS events record – evidence that this record is current and includes all significant events.

10.3. Attach the recertification to the PDS file as shown in [Figure 1.](#)

10.4. A PDS that does not meet the above requirements may not be recertified.

10.4.1. The wing IA office notifies the DAA immediately when a PDS is not recertified.

10.4.2. The PDS is shut down immediately.

10.4.3. The requesting agency corrects deficiencies discovered during recertification within 30 days and requests recertification.

10.4.4. A PDS that fails recertification cannot be used until recertified.

Figure 1. The PDS Package File.



11. Protected Distribution System Deactivation . The operating agency reports deactivation of an approved PDS to the DAA and wing IA office within 5 days of deactivation. Destroy all files pertaining to the deactivated PDS after 90 days.

12. Information Collections, Records, and Forms .

12.1. Information Collections. No information collections are created by this publication.

12.2. Records. Maintain and dispose of program records in accordance with AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322 Volume 4), Table 33-22, Rule 13.

12.3. Forms. No forms are prescribed by this publication.

JOHN L. WOODWARD, JR., Lt General, USAF
DCS, Communications and Information

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

NSTISSI 7000, (C) *TEMPEST Countermeasures for Facilities (U)*, Annex A, (S) *TEMPEST Threat to Facilities (U)*

NSTISSI 7003, *Protected Distribution Systems*

National Security Agency Information Systems Security Products and Services Catalog

AFPD 33-2, *Information Protection* (will convert to Information Assurance)

AFI 31-101, (FOUO) *The Air Force Installation Security Program*

AFI 33-103, *Requirements Development and Processing*

AFI 33-201, (FOUO) *Communications Security (COMSEC)*

AFI 33-212, *Reporting COMSEC Deviations*

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-322 Volume 4)

AFDIR 33-303, *Compendium of Communications and Information Terminology*

AFSSI 5024, Volume I, *The Certification and Accreditation (C&A) Process*

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigation

AFPD—Air Force Policy Directive

C&A—Certification and Approval

CAA—Controlled Access Area

COMSEC—Communications Security

CSO—Communications and Information Systems Officer

DAA—Designated Approving Authority

dB—Decibels

EMSEC—Emission Security

EMT—Electrical Metallic Tubing

FOUO—For Official Use Only

GSA—Government Services Administration

IA—Information Assurance

IDOCS—Intrusion Detection Optical Communications System

LCA—Limited Controlled Area

MAJCOM—Major Command

MHz—Megahertz

NSA—National Security Agency

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

OTDR—Optical Time Domain Reflectometry

PDS—Protected Distribution System

PVC—Polyvinyl Chloride

SCIF—Sensitive Compartmented Information Facility

SPECAT—Special Category

STEM—Systems Telecommunications Engineering Manager

STP—Shielded Twisted-Pair

TDR—Time Domain Reflectometry

UAA—Uncontrolled Access Area

Terms

Access Control—Process of limiting access to the resources of an information system (IS) only to authorized users, programs, processes, or other systems.

Controlled Access Area (CAA)—The complete building or facility area under direct physical control within which unauthorized persons are denied unrestricted access and are either escorted by authorized persons or are under continuous physical or electronic surveillance.

Limited Controlled Area (LCA)—The space surrounding a protected distribution system within which exploitation is not considered likely or legal authority to identify or remove a potential exploitation exists.

Protected Distribution System (PDS)—A wire line or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified national security information. **NOTE:** This definition does not include intrusion detection optical communications systems (IDOCS) approved by the National Security Agency.

Special Category (SPECAT)—The definition is classified (see AFSSI 7010 [S] will convert to AFMAN 33-214 Volume 1[S]).

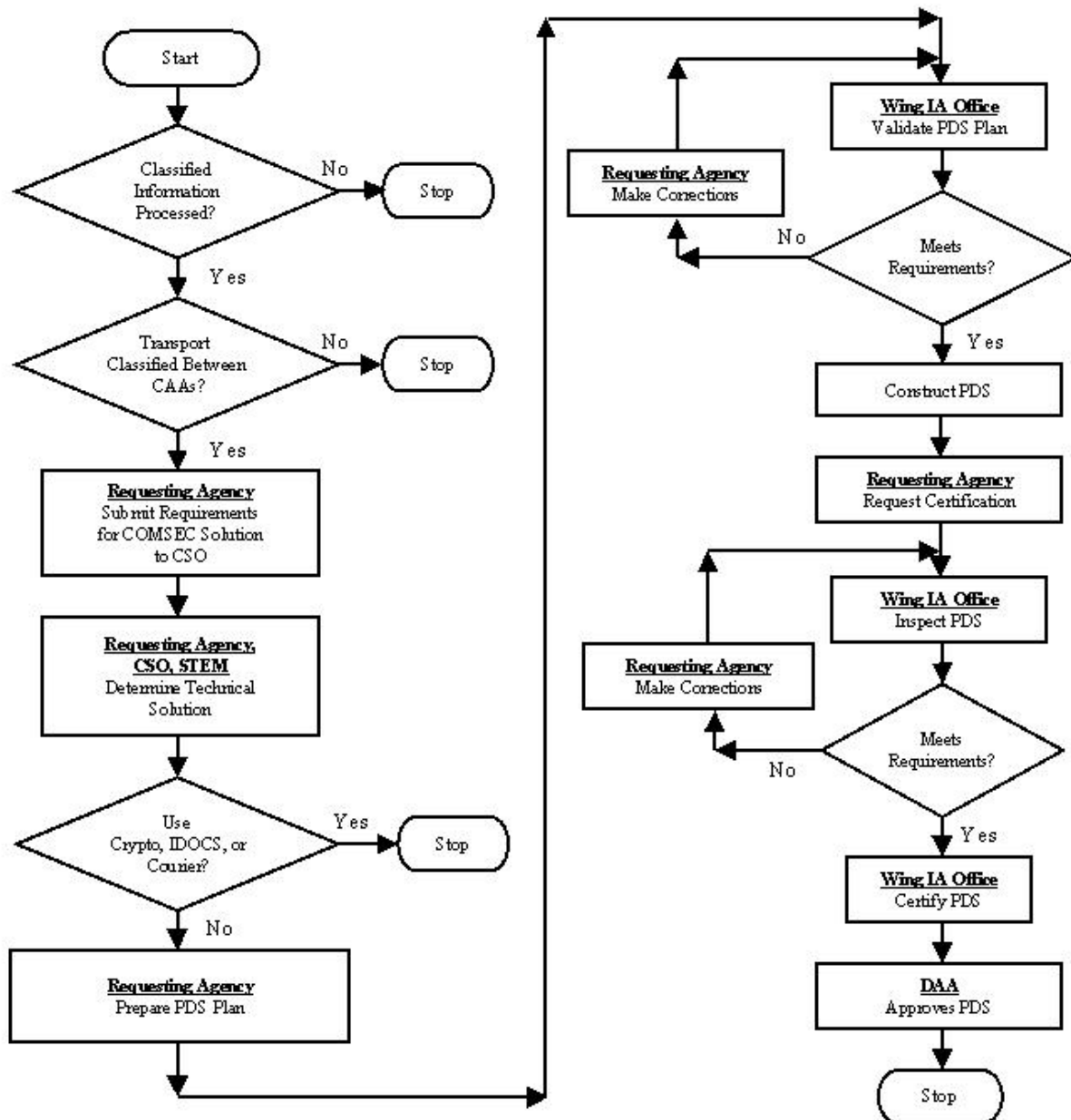
Uncontrolled Access Area (UAA)—The area external or internal to a facility over which no personnel access controls can be or are exercised.

Attachment 2

PROTECTED DISTRIBUTION SYSTEMS PROCESS FLOW CHART

A2.1. Figure A2.1 is a flow chart of the process to design, construct, and approve a PDS.

Figure A2.1. The PDS Plan, Validation, Construction, Certification, and Approval Process.



Attachment 3**PROTECTED DISTRIBUTION SYSTEMS OPERATION REQUIREMENTS**

A3.1. Introduction . This attachment identifies the operation requirements needed to ensure and maintain the security of the PDS. The operation requirements listed in this attachment are the minimum requirements. Meet each requirement with an official memorandum, a letter of appointment, an operating instruction, or other official means.

Controlling Office. Identify the office responsible for controlling the PDS (may be the same as the security office or the record office). Neither the MAJCOM nor the wing IA office will be identified as the controlling office. This office is responsible for all aspects of the PDS except final approval to operate which is a responsibility of the DAA.

A3.1.1. Establish the operational security procedures for the PDS. Draft procedures are permitted for validation (see paragraph 6.). Finalize them for certification (see paragraph 8.).

A3.1.2. Establish the requirement for all personnel in the CAAs to be aware they are responsible to assist in the close supervision of the visible components of the PDS. They are to report all incidents of suspicious activity immediately.

A3.2. Security Office . Identify a PDS security office or person (may be the same as the controlling office or the record office). Neither the MAJCOM nor the wing IA office will be identified as the security office. This office or person will:

A3.2.1. Review the PDS log at least monthly.

A3.2.2. Receive reports of alarms (if used) and incidents of tampering, penetration, or unauthorized interception, immediately make the initial investigation, and resolve or notify the specified investigating agency such as security forces, Air Force Office of Special Investigations (AFOSI), etc.

A3.2.3. Receive reports of suspicious activity in the area of the PDS, immediately make the initial investigation, and resolve or report such activities to security forces for appropriate action.

A3.2.4. Make required notifications.

A3.3. Record Office . Specify the office, or person, to maintain a record of events for the PDS (may be the same as the controlling office or the security office). Neither the MAJCOM nor the wing IA office will be identified as the record office. Record all PDS events such as alarms, lines route inspections, technical inspections, employee reports, and so forth.

A3.4. Reporting Procedures . Establish the procedures for reporting incidents of tampering, penetration, or unauthorized interception. These incidents will most likely be discovered during lines route inspections and technical inspections. Ensure these incidents are reported immediately. Specify the means for reporting such as secure telephone, in person, etc. Include the requirement to discontinue using the PDS until the approval authority assesses the incident and its security status is determined.

A3.4.1. Immediately report these incidents to the PDS security office, or person, for review and initiation of an investigation.

A3.4.2. Immediately report these incidents as a physical security COMSEC incident following the procedures established for physical security incidents in AFI 33-212, *Reporting COMSEC Deviations*.

A3.5. Investigating Procedures . Establish the procedures for investigating reports of tampering, penetration, or unauthorized interception. This should involve the Air Force Office of Special Investigation (AFOSI) since these incidents could be acts of espionage.

A3.6. Monitoring Alarms . If the PDS is alarmed, identify who will monitor the alarm indicator.

A3.7. Responding to Alarms . If the PDS is alarmed, establish the requirement to respond to an alarm within 5 minutes and identify the individuals responding.

A3.8. Investigating Alarms . If the PDS is alarmed, identify who will initially investigate alarms to determine if an attempt at tampering, penetration, or unauthorized interception is suspected. If an attempt is suspected, notify the specified investigating agency; typically, this is the AFOSI.

Attachment 4

PROTECTED DISTRIBUTION SYSTEMS PHYSICAL SECURITY REQUIREMENTS

A4.1. General . This attachment provides requirements for selecting the appropriate type of distribution system to provide the required physical security for the signal line. The intent of operational security procedures in combination with construction requirements allows for rapid detection of any attempted penetration of the PDS rather than ensuring the prevention of a penetration. Varying degrees of protection are based on the PDS construction and other physical protection measures incorporated.

A4.2. Determine Type of Distribution System . Using the highest level of information, or special category (SPECAT) information, and the type of area to be traversed by the PDS (uncontrolled access area [UAA], limited controlled area [LCA], or CAA), determine the required type of distribution system (hardened or simple) from [Table A4.1.](#) and [Table A4.2.](#)

Table A4.1. Required Type of Distribution Systems within the U.S. and Outside the U.S. – Low Threat.

	Type of Area TRAVERSED				
TYPE OF DATA	UAA	LCA	CONFIDENTIAL CAA	SECRET CAA	TOP SECRET CAA
CONFIDENTIAL	Hardened	Simple	Note 1	Note 1	Note 1
SECRET	Hardened	Simple	Simple	Note 1	Note 1
TOP SECRET	Hardened	Hardened	Simple	Simple	Note 1
SPECAT	Hardened	Hardened	Simple	Simple	Simple
1 PDS not required, consider as a RED signal line within the CAA.					

Table A4.2. Required Type of Distribution Systems Outside the U.S. – Medium Threat.

	Type of Area TRAVERSED				
TYPE OF DATA	UAA	LCA	CONFIDENTIAL CAA	SECRET CAA	TOP SECRET CAA
CONFIDENTIAL	Hardened	Simple	Note 1	Note 1	Note 1
SECRET	Hardened	Hardened	Simple	Note 1	Note 1
TOP SECRET	Hardened	Hardened	Hardened	Simple	Note 1
SPECAT	Hardened	Hardened	Hardened	Simple	Simple
1 PDS not required, consider as a RED signal line within the CAA.					

A4.3. Hardened Distribution System . If a hardened distribution system is required, identify the type of carrier (hardened, alarmed, or continuously viewed) to be used.

A4.3.1. Hardened Carrier. If a hardened carrier was chosen:

A4.3.1.1. All security requirements must be enforced 24 hours a day, 7 days a week, whether the PDS is in continuous operation or not.

A4.3.1.2. When designing and installing a hardened carrier, do not conceal it from view by placing it behind walls, above ceilings, or below floors. If you want to conceal the carrier from view, you must use an alarmed carrier. Within the United States, you may encase the carrier in concrete in lieu of alarming the carrier. The concrete encasement must be a minimum of 20 centimeters in all directions.

A4.3.1.3. Secure the termination when the network security policy requires it. Normally, you are required to secure the termination when the termination is not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours a day, 7 days a week. This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a Sensitive Compartmented Information Facility [SCIF]). There are several solutions; one of which is to shut down the circuit to the unattended terminal. Another solution is to use a lockbox. A lockbox is a metallic box attached to the end of the PDS within the CAA large enough to hold the signal line.

A4.3.1.4. Identify the lines route inspection requirements.

A4.3.1.4.1. Identify the required minimum interval for lines route inspections from **Table A4.3.** (this information, when applied to a specific PDS, is For Official Use Only [FOUO]). Daily inspections must be made on weekends and holidays.

A4.3.1.4.2. Specify the office that will make the lines route inspections.

A4.3.1.4.3. A lines route inspection consists of a close visual inspection of the PDS for signs of penetration, tampering, and any other anomaly that may cause a deterioration of protection safeguards. The close visual inspection must include the total surface (360 degrees) of the PDS (especially those parts close to walls and so forth); use of a mirror is recommended. If the PDS is buried, the close visual inspection must extend 5 meters on either side of the PDS route; you are looking for evidence of unauthorized digging.

A4.3.1.4.4. The persons selected to accomplish the route inspections need not be qualified installers or technicians, but they must know enough about the PDS construction to recognize physical changes in the PDS including attempts at penetration and tampering.

Table A4.3. PDS Lines Route Inspection Schedule.1

	Facility Location					
Highest Classification OF Data Carried	WITHIN THE U.S.		OUTSIDE THE U.S. LOW THREAT ²		OUTSIDE THE U.S. MEDIUM THREAT ²	
	UAA	LCA	UAA	LCA	UAA	LCA
SPECAT or Top Secret	2	1	2	1	6	3
Secret	1	13	1	13	4	2
Confidential	1	None	1	None	2	1
1 Minimum number of randomly scheduled inspections per day per location, unless specified as weekly or monthly.						
2 The threat environment is defined by NSTISSI 7000, (C) <i>TEMPEST Countermeasures for Facilities</i> (U), Annex A, (S) <i>TEMPEST Threat to Facilities</i> (U).						
3 For buildings that are secured when not occupied (nights and weekends); lines route inspections may be accomplished on a weekly basis.						

A4.3.1.5. Identify the technical inspection requirements.

A4.3.1.5.1. Identify the minimum interval to make technical inspections from [Table A4.4.](#) (this information, when applied to a specific PDS, is FOUO).

A4.3.1.5.2. Specify the office or organization that will make the technical inspections or ensure inspection completion. Technical inspection requirements are defined in [Attachment 8.](#)

Table A4.4. PDS Technical Inspection Schedule.1

	Facility Location		
HIGHEST Classification of Data Carried	WITHIN THE U.S.	OUTSIDE THE U.S. LOW THREAT ²	OUTSIDE THE U.S. MEDIUM THREAT ²
SPECAT or Top Secret	1	1	4
Secret	1	1	2
Confidential	1	1	1
1 Minimum number of randomly scheduled technical inspections per year.			
2 The threat environment is defined by NSTISSI 7000, (C) <i>TEMPEST Countermeasures for Facilities</i> (U), Annex A, (S) <i>TEMPEST Threat to Facilities</i> (U).			

A4.3.2. Alarmed Carrier. Use an alarmed carrier when the carrier is routed through an area that does not allow unrestricted visual inspection (above suspended ceilings, in walls, below raised floors). If an alarmed carrier is chosen:

A4.3.2.1. All security requirements must be enforced 24 hours a day, 7 days a week whether the PDS is in continuous operation or not.

A4.3.2.2. Identify the office to monitor the PDS alarm, 24 hours a day, 7 days a week.

A4.3.2.3. Specify the required responses to alarm conditions (this information, when applied to a specific PDS, is FOUO).

A4.3.2.4. Identify the office that will respond to PDS alarms.

A4.3.2.5. Establish the required minimum interval for alarm circuit verification from [Table A4.5](#). (this information, when applied to a specific PDS, is FOUO).

Table A4.5. Alarm Circuit Verification Schedule.

Highest Classification of Data Carried	INTERVAL
SPECAT or Top Secret	Monthly
Secret	Quarterly
Confidential	Quarterly

A4.3.2.6. Identify the technical inspection requirements.

A4.3.2.6.1. Identify the minimum interval to make technical inspections from [Table A4.4](#). (this information, when applied to a specific PDS, is FOUO).

A4.3.2.6.2. Specify the office or organization that will make the technical inspections or ensure inspection completion. Technical inspection requirements are defined in [Attachment 7](#).

A4.3.2.7. Secure the termination when the network security policy requires it. Normally, you are required to secure the termination when the termination is not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours a day, 7 days a week. This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a SCIF). There are several solutions; one of which is to shut down the circuit to the unattended terminal. Another solution is to use a lockbox. A lockbox is a metallic box attached to the end of the PDS within the CAA large enough to hold the signal line.

A4.3.2.8. Alarmed carriers do not require lines route inspections.

A4.3.3. Continuously Viewed Carrier. If the continuously-viewed PDS is chosen:

A4.3.3.1. All security requirements must be enforced 24 hours a day, 7 days a week whether the PDS is in continuous operation or not.

A4.3.3.2. Identify the office to provide the monitoring service.

A4.3.3.3. A continuously viewed carrier must be under continual observation (24-hours a day, 7 days a week), whether in use or not.

A4.3.3.4. Secure the termination when the network security policy requires it. Normally, you are required to secure the termination when the termination is not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours a day, 7 days a week. This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a SCIF). There are several solutions; one of which is to shut down the circuit to the unattended terminal. Another solution is to use a lockbox. A lockbox is a metallic box attached to the end of the PDS within the CAA large enough to hold the signal line.

A4.3.3.5. Identify the technical inspection requirements.

A4.3.3.5.1. Identify the required minimum interval to make the technical inspections from [Table A4.4](#) (this information, when applied to a specific PDS, is FOUO).

A4.3.3.5.2. Specify the office or organization that will make the technical inspections or ensure inspections are completed. Technical inspection requirements are defined in [Attachment 7](#).

A4.3.3.6. Continuously viewed carriers do not require lines route inspections.

A4.4. Simple Distribution System . This system provides a reduced level of physical protection as compared to the hardened distribution system.

A4.4.1. All security requirements must be enforced 24 hours a day, 7 days a week, whether the PDS is in continuous operation or not.

A4.4.2. When designing and installing a simple carrier, do not conceal it from view by placing it behind walls, above ceilings, or below floors. If you want to conceal the carrier from view, you must provide additional physical security. For a concealed simple carrier within a building, within the United States, do one of the following:

A4.4.2.1. Secure the building when not occupied (nights and weekends). See paragraph [A4.4.4.](#) for lines route inspection requirements and paragraph [A4.4.5.](#) for technical inspection requirements.

A4.4.2.2. Use an alarmed carrier. Follow paragraph [A4.3.2.](#) for alarmed carrier physical security requirements.

A4.4.2.3. Encase the carrier in concrete.

A4.4.3. Secure the termination when the network security policy requires it. Normally, you are required to secure the termination when the termination is not in use and the signal lines from the carrier terminate at a user equipment terminal location not maintained as a CAA 24 hours a day, 7 days a week. This requirement usually does not apply to CAAs accredited for open storage or CAAs in secure facilities (e.g., a SCIF). There are several solutions; one of which is to shut down the circuit to the unattended terminal. Another solution is to use a lockbox. A lockbox is a metallic box attached to the end of the PDS within the CAA large enough to hold the signal line.

A4.4.4. Identify the lines route inspection requirements.

A4.4.4.1. Identify the required minimum interval for lines route inspections from [Table A4.3.](#) (this information, when applied to a specific PDS, is FOUO). Lines route inspections are required for concealed, unalarmed simple carriers in buildings that are secured when not occupied. The intervals are the same for exposed simple carriers in a building that is not secured when unoccupied.

A4.4.4.2. Specify the office that will make the lines route inspections.

A4.4.4.3. A lines route inspection consists of a close visual inspection of the carrier for signs of penetration, tampering, and any other anomaly that may cause a deterioration of protection safeguards. The close visual inspection must include the total surface (360 degrees) of the carrier (especially those parts close to walls, and so forth); use of a mirror is recommended. If the PDS is buried, the close visual inspection must extend to 5 meters either side of the PDS route; you are looking for evidence of unauthorized digging.

A4.4.4.4. The persons selected to accomplish the lines route inspections need not be qualified installers or technicians, but they must know enough about the carrier construction to recognize physical changes in the carrier including attempts at penetration and tampering.

A4.4.5. Identify the technical inspection requirements.

A4.4.5.1. Identify the required minimum interval to make the technical inspections from [Table A4.4](#). (this information, when applied to a specific PDS, is FOUO).

A4.4.5.2. Specify the office or organization that will make the technical inspections or ensure inspections are completed. Technical inspection requirements are defined in [Attachment 7](#).

A4.4.5.3. In buildings that are secured when not occupied and the simple carrier is concealed but not alarmed, you must make a technical inspection whenever there is evidence of a forced or unauthorized entry to the secured building.

A4.5. Tactical Arena .

A4.5.1. In tactical environments, locate the PDS within areas directly under U.S. forces physical control.

A4.5.2. Protect the perimeters or keep under surveillance, with armed guards or patrols, the area surrounding the PDS.

A4.5.3. Provide protection commensurate with the level of information passed through the PDS.

A4.5.4. The responsible commander assesses the risks associated with maintaining the security of the system. Include factors such as stability of the area and technical intelligence collection proficiency of adversaries, to include the host country, and their capability to collect and relay information obtained.

A4.6. Marking a Protected Distribution System . Do not mark a PDS outside the CAA. The COMSEC requirement to mark all RED signal lines with red tape or paint applies only to RED signal lines within the CAA.

Attachment 5

PROTECTED DISTRIBUTION SYSTEM SIGNAL LINE REQUIREMENTS

A5.1. Introduction . This attachment identifies the signal line requirements.

A5.2. Signal Line Requirements . The PDS carrier provides physical security preventing direct access to the signal line. However, wire signal lines are known to emanate the intended signal. Where the PDS is metallic, the intended signal will couple to the PDS carrier providing direct access to the signal. The requirement is to contain any emanations of the intended unencrypted signal within the PDS. Use shielded metallic wire cable, shielded metallic wire lines, or fiber optics. Meet this mandatory requirement as follows: *NOTE:* Do not confuse the requirements to contain emanations of the intended unencrypted signal with Emission Security (EMSEC) countermeasures. Different technical intercept methods are used for the two signal types, EMSEC being more difficult and complex. EMSEC countermeasures are applied to contain unintended compromising emanations within the inspectable space.

A5.2.1. Shielded Wire Lines. Use shielded twisted-pair (STP) or shielded multiconductor wire cable. Each STP or cable must have a minimum of one overall nonferrous shield and must meet the requirements of paragraph [A5.3](#). Ground the shield to a facility signal ground. Keep pigtailed and long ground-wire shield terminations as short as possible. Long pigtailed and terminations drastically reduce shielding effectiveness and, in certain frequency ranges (dependent on pigtail length), can completely nullify the inherent shielding capability of a cable. Crosstalk is permitted on adjacent pairs within a bundle.

A5.2.2. Shielded Coaxial Cables. Typically, the shield of a coaxial cable (outer conductor) is used as a signal return path connected to a signal ground within the equipment. However, the signal ground within the equipment is not necessarily connected to a facility signal ground. When the equipment is not connected to a facility signal ground, the coaxial cable can radiate low-level emanations of the intended signal. In this case, use shielded coaxial (triaxial) cable. Use a second shield insulated from any metallic carrier portion of the PDS and insulated from the coaxial return path or use triaxial cable. The shielding must meet the requirements of paragraph [A5.3](#). Ground the shield at both ends to a facility signal ground. Keep pigtailed and long ground-wire shield terminations as short as possible. Long pigtailed and terminations drastically reduce shielding effectiveness and, in certain frequency ranges (dependent on pigtail length), can completely nullify the inherent shielding capability of a cable.

A5.2.3. Unshielded Coaxial Cable. Unshielded coaxial cable may be used if the shield is connected to a signal ground within the equipment at both ends of the PDS and, in turn, each equipment's signal ground is connected to a facility signal ground.

A5.2.4. Fiber Optic Cables. Use opaque-clad fiber optic cable. It is not necessary to shield fiber optic cables. A fiber optic cable should not contain a metallic conductor of any type (strength members, armor, or metallic particles in the coloring of the cladding). Such metallic conductors can become fortuitous conductors for compromising emanations. If such cables are used, treat them in the same manner as the shield on shielded wire lines; that is, the metallic component must be grounded at both ends within the CAAs to a facility signal ground.

A5.3. Shielded Cable Requirements .

A5.3.1. Physical Cable Characteristics. There are two ways to shield a cable:

A5.3.1.1. Tinned Copper Braid. The cable has an overall shielding of 85 to 90 percent tinned copper-braid coverage. A drain wire is not required in braided-copper shielded cable.

A5.3.1.2. Foil Wrapped. This form of shielded cable can only be used for voice signals and digital signals below 5,000 bits per second. The foil wraps the cable in an overlapping spiral. The overlaps must be z-locked.

A5.3.2. Electrical Cable Characteristics. Shielding must meet the following requirements:

A5.3.2.1. 100 decibels (dB) from 300 to 15,000 hertz.

A5.3.2.2. 80 dB over the baseband video range up to 5 megahertz (MHz).

A5.3.2.3. 60 dB over the frequency range from one to ten times the basic data rate of the digital signal.

Attachment 6

PROTECTED DISTRIBUTION SYSTEMS CONSTRUCTION REQUIREMENTS

A6.1. General . This attachment provides requirements for designing and constructing a PDS to provide the required physical security of the signal line. It does not provide the requirements for safety standards, local building codes, electrical codes, grounding requirements, and so forth.

A6.2. Design and Construction Objective . The intent of these requirements in combination with operational security procedures is to allow for rapid detection of any attempted penetration of the carrier rather than ensuring the prevention of a penetration. **NOTE:** Take precautions to ensure that general construction practices do not void the security requirements of other paragraphs in this manual.

A6.3. Design Requirements .

A6.3.1. Make diagrams showing the proposed route and all involved CAAs, LCAs, and UAAs.

A6.3.2. Make diagrams identifying other wiring, lines, and electrical equipment located along the proposed route within 1 meter of the proposed PDS.

A6.3.3. Include a listing of materials proposed for use to construct the PDS.

A6.4. Hardened Distribution System . This distribution system must provide significant physical security protection for the signal line and is implemented by either the hardened carrier, alarmed carrier, or the continuously viewed carrier as follows:

A6.4.1. Hardened Carrier. The principal protection concept for a hardened carrier is to provide for unencumbered visual inspections to detect penetration, tampering, or unauthorized access to the signal line within the carrier.

A6.4.1.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors. This requirement is to ensure the detection of any penetration of the carrier and preclude hampering that detection.

A6.4.1.1.1. Provide at least 5 centimeters of clearance from walls; floors; ceilings; other wires, cables, ducts; and material that may obstruct viewing during visual inspections. If a wall, floor, or ceiling is at least 20 centimeters of reinforced concrete, you may secure the carrier flush to the wall, floor, or ceiling instead of leaving a 5-centimeter gap. Flush mounting cannot leave gaps more than 5 millimeters or slack where the carrier could be temporarily pulled away from the surface providing access to the part hidden from view (against the surface). Secure the carrier to the surface at least once every meter for electrical metallic tubing (EMT) or 2 meters for ferrous conduit or pipe or rigid sheet steel ducting. The method for securing the carrier to the surface must either prevent removing and reinstalling a support bracket or clip, or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.4.1.1.2. If the carrier penetrates a wall, ceiling, or floor:

A6.4.1.1.2.1. The carrier must extend unbroken for at least 30 centimeters on either side of the penetration.

A6.4.1.1.2.2. If the carrier is anchored so it cannot be moved back and forth more than 5 millimeters through the hole, you may use minimum clearance. The method for anchoring the carrier must either prevent removing and reinstalling a support bracket or clip, or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.4.1.1.2.2.1. Permanent filler, sealant, or foam may fill the hole.

A6.4.1.1.2.3. If the carrier cannot be anchored so it cannot be moved back and forth no more than 5 millimeters, provide at least 5 centimeters of clearance all the way around the carrier (minimum 10-centimeter hole) for thickness up to 10 centimeters. Double the clearance for each additional 10 centimeters (minimum 20-centimeter hole for 10- to 20-centimeter thickness). Center the carrier in the hole.

A6.4.1.1.2.3.1. No permanent filler, sealant, or foam may fill the hole. A filler (bat insulation for instance) that is easily removed and reinstalled without tools to facilitate lines route inspections may be used.

A6.4.1.1.3. If you want to conceal the carrier from view, you must use an alarmed carrier or, within the United States, you may encase the carrier in concrete in lieu of alarming it. Use approximately 20 centimeters of concrete or a concrete and steel container. Such encasement must be of sufficient size to preclude surreptitious penetration for at least 2 hours as confirmed by laboratory tests. Include test results in the certification application.

A6.4.1.1.4. Within a CAA, consider the distribution system and signal line as a RED signal line, not as a PDS.

A6.4.1.2. Construct the carrier of EMT, ferrous conduit or pipe, or rigid-sheet steel ducting 12 gauge or better, using elbows, couplings, nipples, and connectors of the same material, or polyvinyl chloride (PVC) tubing, schedule 40 or better, encased in concrete. Such encasement must be of sufficient size to preclude surreptitious penetration for at least 2 hours as confirmed by laboratory tests. Include test results in the certification application.

A6.4.1.3. Permanently seal (weld or epoxy) all connections completely around all surfaces. You may use hinged covers for rigid sheet ducting if you weld the hinges and edges or use tamper-proof hinges and fasten with tamper-proof hasps and high security padlocks. When securing the hinged covers with padlocks, position tamper-proof hasps close enough together to cause permanent warping of the cover if an attempt is made to gain access by prying up the cover.

A6.4.1.4. High-security padlocks must meet AFI 31-101, *The Air Force Installation Security Program*, specifications or Government Services Administration (GSA) three-position combination padlock FF-P-110 standards.

A6.4.1.5. If pull boxes are used, construct them of metal welded permanently and completely around all surfaces, 12 gauge or better. Either completely seal (weld or epoxy) the pull box covers around the mating surfaces after construction or use tamper-proof hinges and hasps and secure the pull boxes with a high security padlock. Do not use boxes with prepunched knockouts.

A6.4.1.6. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare metal when attempting to hide unauthorized penetration.

A6.4.1.7. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal, welded permanently and completely around all surfaces, 12 gauge or better, with tamper-proof hinges and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock.

A6.4.1.8. If you bury the carrier, bury it a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or the contractor having control of the PDS. Secure manholes with a high-security padlock. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms. If you are constructing the buried carrier outside the United States, encase it in approximately 20 centimeters of concrete or a concrete and steel container. Such encasement must be of sufficient size to preclude surreptitious penetration for at least 2 hours as confirmed by laboratory tests. Include test results in the certification application. If you wish to use a buried distribution facility for other unclassified signal lines, it must meet the construction requirements for a PDS. You cannot mix classified and unclassified signal lines within the same carrier. One or more separate carriers must be provided for the unclassified signal lines. Within manholes, the PDS carrier must either be extended through the manhole or the ends of the carrier and the RED signal lines must be clearly marked and separated from unclassified signal lines. An inspection of the PDS within the manhole is required each time cleared personnel with the necessary access enter the manhole.

A6.4.1.9. If you suspend the carrier above ground, install the carrier only if the property traversed is owned or leased by the U.S. Government or contractor having control of the PDS. Suspend carriers at least 5 meters above the ground. Provide unimpeded inspection of the installed suspended carrier. Make sure the carrier is clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

A6.4.1.10. Illuminate the carrier.

A6.4.2. Alarmed Carrier. The principal protection concept of an alarmed carrier provides automatic detection of attempts to penetrate, tamper, or access the signal line within the carrier.

A6.4.2.1. Alarmed carriers may be hidden from view. There are two alarming methods:

A6.4.2.1.1. Area Alarm. Apply intrusion detection alarms to the area through which the carrier passes making the area, in effect, a controlled area. Use intrusion detection alarms approved by the cognizant security authority and also meet the criteria in AFI 31-101 for a controlled area at the classification level of the information processed.

A6.4.2.1.2. Carrier Alarm. Use alarms listed on the Approved Alarm Systems for Protected Distribution Systems. This listing is available at <http://www.afca.scott.af.mil/ip/emsec/emsec.htm>. Operational plans and procedures for a carrier alarm will be the same as if the carrier were an alarmed controlled area. Carrier alarms must meet the following requirements:

A6.4.2.1.2.1. When the alarm system fails, it must transmit a line fault message to the annunciator panel.

A6.4.2.1.2.2. Must lend itself to protection from tampering.

A6.4.2.1.2.3. Must be capable of prompt detection of any attack on the area it is designed to protect.

A6.4.2.1.2.4. Must have an annunciator panel in an office manned 24 hours a day, 7 days a week. The office must be capable of notifying responding forces.

A6.4.2.1.2.5. Must be able to register malfunctions.

A6.4.2.1.2.6. Must have a line fault indicator if the alarm system fails.

A6.4.2.2. Include all pertinent alarm information in the PDS plan. An alarm condition must shut down the RED signal line within the alarmed area or the alarmed carrier. You cannot use the signal line until you perform an inspection and determine the reason for the alarm.

A6.4.2.3. Construct the carrier of EMT, ferrous conduit or steel pipe, using elbows, couplings, nipples, and connectors of the same material. Connections and pull boxes need not be sealed. Do not use boxes with prepunched knockouts.

A6.4.2.4. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal welded permanently and completely around all surfaces, 12 gauge or better, with tamper-proof hinges and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock.

A6.4.2.5. If you bury the carrier, bury it a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or the contractor having control of the PDS. Secure manholes with a high security padlock. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms.

A6.4.2.6. If you suspend the carrier above ground, elevate the carrier a minimum of 5 meters. Make sure the carrier is clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

A6.4.3. Continuously Viewed Carrier. To use a continuously viewed carrier, the guard force must keep the circuit under constant observation 24 hours a day, 7 days a week, not just when operational. You may group circuits together if you separate them from all noncontinuously viewed circuits to ensure an open field of view.

A6.4.3.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors.

A6.4.3.2. Standing orders include the requirement to investigate any attempt to disturb the carrier.

A6.4.3.3. Appropriate security personnel investigate the area of attempted penetration within 5 minutes.

A6.4.3.4. This type of carrier cannot be used for TOP SECRET or SPECAT information in any areas outside the United States, nor on property owned or leased by the U.S. Government or the contractor having control of the PDS within the United States.

A6.4.3.5. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal welded permanently and completely around all surfaces, 12 gauge or better, with tamper-proof hinges and tamper-proof hasp.

Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock.

A6.5. Simple Distribution System . This system provides a reduced level of physical protection as compared to the hardened distribution system. When allowed by [Table A4.1.](#) and [Table A4.2.](#), construct the simple distribution system as follows:

A6.5.1. Hardened Carrier. The carrier may use any hardened carrier in existence.

A6.5.2. Simple Carrier:

A6.5.2.1. Do not conceal the carrier from view by placing it behind walls, above ceilings, or below floors. This requirement is to ensure the detection of any penetration of the carrier and preclude hampering that detection.

A6.5.2.2. Provide at least 5 centimeters of clearance from walls; floors; ceilings; other wires, cables, ducts; and material that may obstruct viewing during visual inspections. If a wall, floor, or ceiling is at least 20 centimeters of reinforced concrete, you may secure the carrier flush to the wall, floor, or ceiling instead of leaving a 5-centimeter gap. Flush mounting cannot leave gaps more than 5 millimeters or slack where the carrier could be temporarily pulled away from the surface providing access to the part hidden from view (against the surface). Secure the carrier to the surface at least once every meter for EMT or PVC pipe and every 2 meters for ferrous conduit or pipe or rigid sheet steel ducting. The method for securing the carrier to the surface must either prevent removing and reinstalling a support bracket or clip or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.5.2.3. If the carrier penetrates a wall, ceiling, or floor:

A6.5.2.3.1. The carrier must extend unbroken for at least 30 centimeters on either side of the penetration.

A6.5.2.3.2. If the carrier is anchored so it cannot be moved back and forth more than 5 millimeters through the hole, you may use minimum clearance. The method for anchoring the carrier must either prevent removing and reinstalling a support bracket or clip or allow the lines route inspector to detect if a bracket or clip has been removed and reinstalled.

A6.5.2.3.3. If the carrier cannot be anchored so it cannot be moved back and forth at least 5 millimeters, provide at least 5 centimeters of clearance all the way around the carrier (minimum 10-centimeter hole) for penetrations up to 10 centimeters. Double the clearance for each additional 10 centimeters (minimum 20-centimeter hole for 10- to 20-centimeter thicknesses). Center the carrier in the hole.

A6.5.2.3.4. No permanent filler, sealant, or foam may fill the hole. A filler (bat insulation for instance) that is easily removed for lines route inspections and reinstalled without tools may be used.

A6.5.2.4. Within a CAA, consider the distribution system and signal line as a RED signal line, not as a PDS.

A6.5.2.5. Inside a building within the LCA, construct the carrier of any material (e.g., ferrous conduit, EMT, PVC pipe of at least a schedule-40 grade material, wood, etc.). Outside a building within the LCA, construct the carrier of ferrous conduit or EMT. Spot-weld or epoxy EMT joints.

Use PVC solvent to seal PVC joints. Glue and cross-nail all joints on wooden carriers. Contain access points within the CAA.

A6.5.2.6. If pull boxes are used, either seal by spot welding or epoxy the pull-box covers after construction or use tamper-proof hinges and hasps. Secure the pull boxes with a high-security padlock. Do not use boxes with prepunched knockouts.

A6.5.2.7. Do not paint or cover the carrier with wallpaper or any other covering. Such covering can conceal surreptitious penetration of the carrier. Paint and coverings are easier to match than the bare material when attempting to hide unauthorized penetration. The one exception is a wooden carrier; it may be stained and sealed.

A6.5.2.8. If a lockbox is required, extend the carrier to it using the same construction requirements as the rest of the carrier. Construct the lockbox of metal welded permanently and completely around all surfaces, 12 gauge or better, with tamper-proof hinges and tamper-proof hasp. Permanently mount the box to the facility structure at a location convenient to the terminal and to where the carrier terminates within the CAA. Secure the box cover with a high security padlock.

A6.5.2.9. If you bury the carrier, bury it a minimum of 1 meter below the surface and on property owned or leased by the U.S. Government or the contractor having control of the PDS. Secure manholes with a high security padlock. If specification locks cannot be used, then use a standard locking manhole cover and approved microswitch alarms.

A6.5.2.10. If you suspend the carrier above ground, elevate the carrier a minimum of 5 meters. Make sure the carrier is clear of any obstruction or device that would encroach upon the carrier to facilitate tampering.

A6.5.2.11. If you want to conceal the carrier from view, you must provide additional physical security. For a concealed simple carrier within a building, within the United States, do one of the following:

A6.5.2.11.1. Secure the building when not occupied (nights and weekends).

A6.5.2.11.2. Use an alarmed carrier. Follow paragraph [A6.4.2.](#) for alarmed carrier construction requirements.

A6.5.2.11.3. Encase the carrier in concrete. The concrete encasement must be a minimum of 20 centimeters in all directions or a concrete and steel container. Such encasement must be of sufficient size to preclude surreptitious penetration for at least 2 hours as confirmed by laboratory tests. Include test results in the certification application.

Attachment 7**PROTECTED DISTRIBUTION SYSTEMS CIRCUIT SEPARATION REQUIREMENTS**

A7.1. Circuit Separation Security Criterion . Ensure personnel accessing any circuit within the distribution system have appropriate clearance. Inhibit inappropriate cross connection of circuits.

A7.2. Access Controls for Collateral Circuits .

A7.2.1. Circuits of more than one classification level may use components of a single distribution system.

A7.2.2. Where the sharing of a single distribution system is feasible, the following criteria are mandatory:

A7.2.2.1. Access Points. Access to all points with breakouts of the higher level circuits must be restricted to appropriately cleared personnel. Access points containing classified circuits of different classification levels that do not have breakouts of the higher level circuits can be serviced by lower level cleared personnel when escorted by appropriately cleared personnel.

A7.2.2.2. Termination Boxes. Locate all termination boxes within the CAA.

A7.3. Access Controls for Special Category . Ask the cognizant Special Security Office for criteria and requirements pertaining to access controls for SPECAT.

Attachment 8

PROTECTED DISTRIBUTION SYSTEMS TECHNICAL INSPECTIONS

A8.1. General . This attachment provides requirements for establishing and completing technical inspections of an installed PDS. Conduct technical inspections at the minimum intervals according to **Table A4.4**. Technical inspections must be performed within the intervals specified, but the schedule should remain random and unannounced. The intervals specified in **Table A4.4** are minimum requirements. Sometimes the local threat assessment and risk analysis results may indicate a need for more frequent inspections. In these situations, the DAA should increase the frequency as deemed appropriate.

A8.2. Responsibilities . Ensuring completion of inspections according to the schedule is the responsibility of the activity identified in the PDS plan; this is normally the owning or using activity. The identified organization will either complete the inspections or coordinate with other organizations on base (e.g., wing communications organization) to have appropriately cleared personnel complete the inspection.

A8.2.1. Because of the technical nature of PDS technical inspections, personnel familiar with communications systems installations and maintenance, or similar technical experience and knowledge of electronics, should conduct or assist in conducting the technical inspections.

A8.3. Requirements . Technical inspections consist of a detailed visual inspection of the entire PDS route and an electrical characterization of the PDS.

A8.3.1. The detailed visual inspections should include all components such as terminal boxes, junction boxes, pull boxes, associated box covers and cover gaskets, manhole access points, connections, connectors, amplifiers, line conditioning equipment, distribution frame connections, optical transmitters, optical receivers, ground connections, locks, lock hasps, hinges, and lock mechanisms.

A8.3.1.1. Open and inspect every manhole cover, locked terminal box, and other locations where locks are used to secure access points. Change all lock combinations as part of the inspection. Record and store lock combinations according to established directives. Report instances of inoperative locks as a physical security COMSEC incident according to AFI 33-212 and the established reporting procedures.

A8.3.1.2. Accomplish an initial technical inspection at the completion of the PDS installation. Personnel of the installing activity assisted by personnel from the activity identified to perform the continuing inspections should accomplish this. During the initial inspection, take photographs of the PDS to document the physical configuration. Pay particular attention to any terminal boxes, junction boxes, pull boxes, manhole access points, and any other areas where access to the PDS cables or wiring may be possible. Ensure each photograph is marked as to the exact position or location of the area photographed. You may devise any system of labeling which will provide for the positive identification of the location shown in the photograph. Narratives that further describe the area shown should also accompany these photographs.

A8.3.1.3. Place the photographs and accompanying narratives in the completed PDS file for use during subsequent inspections to assist in identification of possible tampering. A compilation of photographs, when identified with a specific PDS or system and location may be classified. In all cases, handle, mark, and store as sensitive information.

A8.3.1.4. During the subsequent technical inspections look for changes in the technical aspects of the PDS (e.g., by-pass circuitry, attachment or removal of devices or components, inappropriate or suspicious signal levels, and mechanical integrity of the PDS).

A8.3.2. The electrical characterization consists of such things as time domain reflectometry (TDR) on wire lines and optical time domain reflectometry (OTDR) on fiber optic signal lines. Measure and record the electrical characteristics of the PDS lines to obtain a baseline electrical profile of the PDS. Accomplish the electrical characterization immediately upon completion of the PDS installation. Such measurements may consist of signal levels, voltage levels, TDR recorded readings, and any other electrical measurements that may be recorded and retained. Use a characterization method that will allow use of locally available test equipment and is within the capabilities of the local operating and maintaining function for conducting subsequent technical inspections. Record and compare measurements taken at subsequent technical inspections to the previously recorded baseline measurements to aid in identifying possible tampering attempts.